

⑩ 日本国特許庁(JP)

⑪ 特許出願公開

⑫ 公開特許公報(A) 平4-165785

⑬ Int. Cl.<sup>3</sup>

H 04 N 7/16  
5/44  
7/167

識別記号

C  
K

庁内整理番号

8324-5C  
7037-5C  
8324-5C

⑭ 公開 平成4年(1992)6月11日

審査請求 未請求 請求項の数 1 (全7頁)

⑮ 発明の名称 有料放送受信機

⑯ 特 願 平2-293301

⑰ 出 願 平2(1990)10月29日

⑱ 発 明 者 北 川 和 雄 神奈川県横浜市磯子区新杉田町8 株式会社東芝横浜事業  
所家電技術研究所内

⑲ 出 願 人 株 式 会 社 東 芝 神奈川県川崎市幸区堀川町72番地

⑳ 代 理 人 弁 理 士 伊 藤 進

明 細 書

1. 発明の名称

有料放送受信機

2. 特許請求の範囲

所定の初期値に基づいて作成された疑似ランダム系列と音声データとの排他的論理和演算によって前記音声データにスクランブルを施し、少なくとも受信端末のアドレスを示すID番号、個別契約情報及び前記初期値を含んだ情報を暗号化して前記スクランブルが施された音声データに重畳して送信する送信機からのデータをデスクランブルする有料放送受信機において、

受信端末のアドレスを示すID番号及び個別契約情報を格納する記憶手段と、

前記音声データに重畳されている情報に含まれるID番号と前記記憶手段に格納されたID番号とを比較して契約された番組の情報のみを取出す複数の情報抽出手段と、

この複数の情報抽出手段からの情報を復号する復号手段と、

この復号手段が復号した情報に含まれる前記初期値に基づいて複数の送信局で作成した疑似ランダム系列と同一の複数の疑似ランダム系列を発生する疑似ランダム系列発生器と、

受信された複数のデータと前記疑似ランダム系列発生器からの複数の疑似ランダム系列との排他的論理和演算によって各スクランブルデータをデスクランブルする複数の排他的論理和手段とを具備したことを特徴とする有料放送受信機。

3. 発明の詳細な説明

〔発明の目的〕

〔産業上の利用分野〕

本発明は有料放送受信機に関し、特に、スクランブルされたデジタル音声データをデスクランブルする有料放送受信機に関する。

〔従来の技術〕

1990年4月からは、有料放送を主体とした衛星放送が開始されるようになっている。このような有料放送システムにおいては、未契約者による盗視聴を防止するために、信号にスクランブ

ルを施して送信し、端末受信機においてこのスクランブルを解くことにより正常な信号を再現する方式が採用される。音声信号については、盗聴を困難にするために、ディジタルデータに変換した後にスクランブルを施している。

第3図はこのようなスクランブル音声データを送出する送信側装置を示すブロック図である。この装置は電気通信技術審議会の答申諮同第17号に示されており、第3図ではその映像系が省略されている。

入力端子1を介して入力される音声データは排他的論理和加算器2に与えられる。排他的論理和加算器2は音声用疑似ランダム系列発生器(以下、APNGという)3からのPNパターンと音声データとの排他的論理和演算を行うことによって、音声データにスクランブルを施してスクランブル音声データをスイッチ4の端子aに出力する。APNG3は初期値発生器5からの初期値KSに基づいて、PNパターンを作成している。初期値発生器5は約1秒の略一定周期(TS)毎に、初期

値KSを発生している。

この初期値KSを受信側へ送出することで、受信側においてAPNG3からのPNパターンと同一のPNパターンを作成してデスクランブルを行っている。この初期値KSは番組情報パケットの一部として送出される。この番組情報パケットは未契約者による盗聴を防止するために暗号化されている。すなわち、初期値KS及び局識別コード等によって構成される番組情報パケットは暗号器6に与えられて暗号化される。この場合、暗号器6は長周期鍵KWに基づいて暗号化を行っている。この長周期鍵KWは、契約された受信端末のアドレスを示すID番号及び契約テーブルのデータと共に個別情報パケットを構成している。個別情報パケットは暗号器7に与えられて暗号化される。この場合、暗号器7は個別IDに個々に対応した個別暗号鍵KJに基づいて暗号化を行っており、大きなセキュリティが得られている。

暗号器6、7の出力は夫々スイッチ4の端子b、cに与えられ、スイッチ4からは番組情報パケッ

ト及び個別情報パケットが重畳されたスクランブル音声データが出力される。

第4図は従来の有料放送受信機の構成を示すブロック図である。

受信側装置はパケット分離部12及びセキュリティ部13によって構成されている。入力端子11を介して入力されるスクランブル音声データには番組情報パケット及び個別情報パケットが重畳されている。パケット分離部12は入力データをスクランブル音声データと番組情報パケットと個別情報パケットとに分離してスクランブル音声データを排他的論理和加算器14に与える。

一方、番組情報パケットはセキュリティ部13の番組バッファ15を介して制御CPU16に与えられ、個別情報パケットは個別バッファ17を介してID比較器18に与えられる。個別情報パケットがID比較器18によって個別のアドレスに相当するID番号と比較されることによって、個別情報パケットのうち契約したパケットデータのみが制御CPU16に与えられる。

メモリ21には、受信端末のID番号及び個別暗号鍵KJが格納されており、制御CPU16は、復号部19において、メモリ21から読出した個別暗号鍵KJによって個別情報パケットを復号する。これにより、制御CPU16は、局、有効期限及び長周期鍵KW等を含む契約テーブルを作成して契約テーブルメモリ20に記憶させる。また、受信チャンネルについて放送局との契約が行われている場合には、復号部19は契約テーブルメモリ20に格納された長周期鍵KWによって番組情報パケットを復号する。こうして得られた番組情報パケットから初期値KSが取出され、APNG22及び映像用疑似ランダム系列発生器(以下、VPNGという)23に与えられる。

なお、契約テーブルメモリ20及びメモリ21は、電池でバックアップされたRAM又はEEPROM等の不揮発性メモリによって構成される。

APNG22は、送信側でAPNG3(第3図参照)が発生したPNパターンと同一のPNパターンを発生して排他的論理和加算器14に与える。排

他の論理和加算器14はこのPNパターンとスクランブル音声データとの排他的論理和演算を行うことにより、スクランブル音声データをデスクランブルして出力する。なお、VPNG23からのPNパターンは図示しないビデオデスクランブル回路に与えられる。

ところで、上述したように、セキュリティ部13は復号部19、APNG22及び契約テーブルメモリ20等を有していることから、不正視聴に対して放送局側を保護するために、通常1チップICか又はモジュールの形態で構成される。このような構成においては、2チャンネル以上の番組を同時にデスクランブルすることはできない。したがって、通常のビデオテープレコーダとテレビジョン受信機との組み合わせのように、視聴中のチャンネル以外のチャンネルを録画する、所謂、裏録を衛星有料放送で行うためには、2台の受信機を必要とする。しかしながら、ID番号が同一の受信機を複数台生産し、同一ID番号の受信機が一戸の家に設置されるように管理することは極めて困難であ

う。一方にスクランブルを施し、少なくとも受信端末のアドレスを示すID番号、個別契約情報及び前記初期値を含んだ情報を暗号化して前記スクランブルが施された音声データに重畳して送信する送信機からのデータをデスクランブルする有料放送受信機において、受信端末のアドレスを示すID番号及び個別契約情報を格納する記憶手段と、前記音声データに重畳されている情報に含まれるID番号と前記記憶手段に格納されたID番号とを比較して契約された番組の情報のみを取出す複数の情報抽出手段と、この複数の情報抽出手段からの情報を復号する復号手段と、この復号手段が復号した情報に含まれる前記初期値に基づいて複数の送信局で作成した疑似ランダム系列と同一の複数の疑似ランダム系列を発生する疑似ランダム系列発生器と、受信された複数のデータと前記疑似ランダム系列発生器からの複数の疑似ランダム系列との排他的論理和演算によって各スクランブルデータをデスクランブルする複数の排他的論理和手段とを具備したものである。

る。すなわち、ユーザーは同一のID番号及び個別暗号鍵K<sub>n</sub>の2台の受信機を得ることはできず、2チャンネルを同時に受信するためには、2重契約を結ぶ必要もあるという問題点があった。

(発明が解決しようとする課題)

このように、上述した従来の有料放送受信機においては、2チャンネル以上の番組を同時にデスクランブルすることができないことから、裏録を行う場合には、2台の受信機を必要とすると共に、2重契約を結ぶ必要もあるという問題点があった。

本発明はかかる問題点に鑑みてなされたものであって、同時に2チャンネル以上の番組をデスクランブルすることができる有料放送受信機を提供することを目的とする。

[発明の構成]

(課題を解決するための手段)

本発明に係る有料放送受信機は、所定の初期値に基づいて作成された疑似ランダム系列と音声データとの排他的論理和演算によって前記音声デ

(作用)

本発明においては、複数の情報抽出手段によって、契約されている番組の情報が抽出される。この情報は復号手段によって複合される。情報には初期値が含まれており、複数の疑似ランダム系列発生器は各受信チャンネルに対応した疑似ランダム系列を発生する。複数の排他的論理和手段はスクランブルされている各受信データと各疑似ランダム系列との排他的論理和演算を行って、各受信データをデスクランブルして出力する。

(実施例)

以下、図面を参照して本発明の実施例について説明する。第1図は本発明に係る有料放送受信機の一実施例を示すブロック図である。第1図において第4図と同一の構成要素には同一符号を付してある。本実施例は2チャンネルの有料放送データを同時にデスクランブルすることができるようにしたものである。

入力端子31、32には番組情報パケット及び個別情報パケットが含まれたスクランブル音声データ

が入力される。これらのスクランブル音声データは異なるチャンネルの放送信号を受信して得たものであり、夫々パケット分離部12, 33に与えられる。パケット分離部12, 33はいずれも同一構成であり、入力されたデータからスクランブル音声データと番組情報パケットと個別情報パケットとを分離する。パケット分離部12, 33からのスクランブル音声データは夫々排他的論理和加算器14, 34に与えられ、番組情報パケットは夫々セキュリティ部35の番組バッファ15, 36を介して制御CPU 37に与えられ、個別情報パケットはいずれも個別バッファ38を介してID比較器39に与えられる。

ID比較器39は個別情報パケットに含まれるID番号と受信機の個別のアドレスに相当するID番号とを比較することにより、契約している番組の個別情報パケットのみを制御CPU 37に与える。制御CPU 37は復号部19、メモリ21及び契約テーブルメモリ20を制御して送信側でPNパターンの発生に使用した初期値KSを再生するようになっている。メモリ21には、各受信機毎に設定された

ID番号及び個別暗号鍵K<sub>0</sub>が納されている。復号部19は制御CPU 37に制御されて、個別暗号鍵K<sub>0</sub>を使用して個別情報パケットを復号し、局、有効期限及び長周期鍵KW等を含む契約テーブルを作成する。契約テーブルメモリ20は復号部19によって作成された契約テーブルを格納するようになっている。

また、復号部19は、受信番組について放送局との契約が行われている場合には、契約テーブルメモリ20に格納された長周期鍵KWに基づいて番組情報パケットを復号する。制御CPU 37は、複合された番組情報パケットから初期値KSを取り出し、APNG 22, 40及びVPNG 23, 41に与えるようになっている。

APNG 22, 40は、送信側でスクランブル時に発生したPNパターンと同一のPNパターンを発生して夫々排他的論理和加算器14, 34に与える。排他的論理和加算器14, 34はこれらのPNパターンと各受信チャンネルのスクランブル音声データとの排他的論理和演算を行うことにより、スクラ

ンブル音声データをデスクランブルして出力端子42, 43に出力する。なお、VPNG 23, 41からのPNパターンは図示しないビデオデスクランブル回路に与えられるようになっている。

次に、このように構成された有料放送受信機の動作について説明する。

入力端子31, 32には異なるチャンネルのスクランブル音声データが入力される。これらの音声データには番組情報パケット及び個別情報パケットが重畳されており、パケット分離部12, 33において分離される。これらの音声データは、通常、TS秒(略1秒)の周期で入力されており、パケット分離部12, 33により十分にパケット処理可能である。パケット分離部12, 33で分離された個別情報パケットは個別バッファ38を介してID比較器39に与えられ、受信機に設定された個別のID番号と比較される。

個別情報パケットは数回/月の頻度で送出されており、2つのチャンネルの個別情報パケットが同時に入力される確率は極めて低い。したがって、

1系統の個別バッファ38で処理可能である。また、2つの受信チャンネルの個別情報パケットが同時に端子31, 32から入力されて個別情報パケットを取込むことができない場合でも、個別情報パケットは1月に1回取込めばよいので、特に問題はならない。この場合には、個別情報パケットが送られてくることにより、電源オフと同一の状態となる。

個別情報パケットはID比較器39を介して制御CPU 37に与えられ、復号部19によって、個別暗号鍵K<sub>0</sub>に基づいて復号される。こうして、契約テーブルメモリ20には局、有効期限及び長周期鍵KW等が格納される。

一方、番組情報パケットは番組バッファ15, 36を介して制御CPU 37に与えられる。制御CPU 37は、受信した番組が放送局と契約されている場合には、契約テーブルメモリ20に格納された長周期鍵KWに基づいて番組情報パケットを復号させる。制御CPU 37は複合した番組情報パケットから初期値KSを取り出して、APNG 22, 40及びV

PNG 23, 41に与える。APNG 22, 40は夫々初期値KSに基づいてPNパターンを作成して排他的論理和加算器14, 34に与える。排他的論理和加算器14, 34はスクランブル音声データとPNパターンとの排他的論理和演算を行って、デスクランブルした音声データを夫々出力端子42, 43に出力する。VPNG 23, 41からのPNパターンは図示しないビデオデスクランブル回路に与えられて、映像データのデスクランブルに使用される。

なお、APNG 22, 40及びVPNG 23, 41がPNパターンを作成するために、初期値KSを使用するタイミングは約TS/2秒であり、制御CPU 37で充分処理可能である。例えば、制御CPU 37として6MHzで動作するZ80を使用した場合には、約5m秒以内にデスクランブル処理が可能である。

このように、本実施例においては、2系統のAPNG 22, 40及びVPNG 23, 41を使用することにより、2つのチャンネルのデータを同時にデスクランブルすることを可能にしている。これによ

ていることを示すモード信号が与えられた場合にはオフとなり、パケット分離部12からの個別情報パケットを個別／番組バッファ48に与えない。この場合には、モード信号によってID比較器49は比較動作を停止し、入力されたパケット分離部33からの番組情報パケットをそのまま通過させて制御CPU 50に与えるようになっている。制御CPU 50は復号部19、メモリ21及び契約テーブルメモリ20を使用して初期値KSを求めて、APNG 22及びV/APNG 51に与えるようになっている。

V/APNG 51は、制御CPU 50から初期値KSが与えられて通常のテレビジョン放送の映像データ用のPNパターンを発生すると共に、モード信号によってPCM音声マルチ放送が受信されていることが示された場合には、動作クロックが切換えられて（図示省略）、音声データ用のPNパターンを発生するようになっている。

次に、このように構成された実施例の動作について説明する。

いま、PCM音声マルチ放送が受信されている

り、2台の受信機を用意することなく、また、2重契約を結ぶことなく衛星有料放送の裏録が可能である。

第2図は本発明の他の実施例にかかる有料放送受信機を示すブロック図である。第2図において第1図と同一の構成要素には同一符号を付して説明を省略する。

本実施例は、通常のテレビジョン放送と、音声のみのPCMマルチ放送との両用受信機に適用したものである。入力端子31には通常のテレビジョン放送の受信スクランブル音声データが入力され、入力端子32にはPCMマルチ放送の受信スクランブル音声データが入力されるようになっている。セキュリティ部45は端子46を介して入力されるモード信号によって制御される。パケット分離部12からの個別情報パケットはスイッチ47を介して個別／番組バッファ48に与えられ、パケット分離部33からの番組情報パケットは直接個別／番組バッファ48に与えられる。

スイッチ47はPCM音声マルチ放送が受信され

ものとする。この場合には、端子46からのモード信号によって、スイッチ47はオフとなり、個別／番組バッファ48は番組バッファとして機能する。また、ID比較器49はパケット分離部33からの番組情報パケットをそのまま通過させて制御CPU 50に与える。こうして、制御CPU 50は初期値KSを作成してAPNG 22及びV/APNG 51に与える。この場合には、モード信号によって、V/APNG 51のクロックが切換えられてV/APNG 51は音声データ用のPNパターンを発生する。

APNG 22及びV/APNG 51からのPNパターンは夫々排他的論理和加算器14, 34に与えられ、排他的論理和加算器14, 34は排他的論理和演算によってデスクランブルした音声データを出力端子42, 43に出力する。

このように、本実施例においては、通常のテレビジョン放送の映像データ用のVPNGを音声用のAPNGとして共用すると共に、個別バッファと番組バッファとを共用し、音声に関しては通常のテレビジョン放送とPCMマルチ放送のデスク

ランブルを可能にしている。これにより、第1図の実施例と同様の効果を得ることができると共に、ハード規模を殆ど増加させることなく、2つのチャンネルの音声データを同時にデスクランブルすることができる。

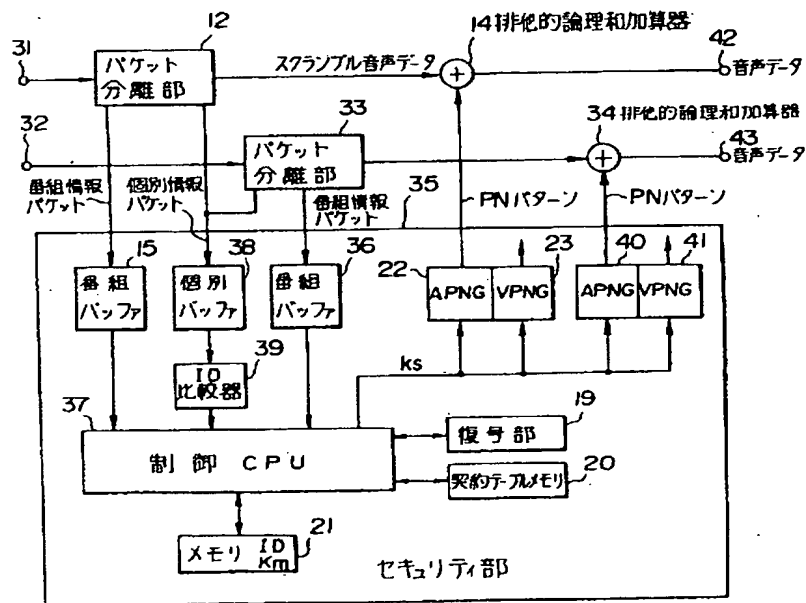
#### 〔発明の効果〕

以上説明したように本発明によれば、同時に2チャンネル以上の番組をデスクランブルすることができるという効果を有する。

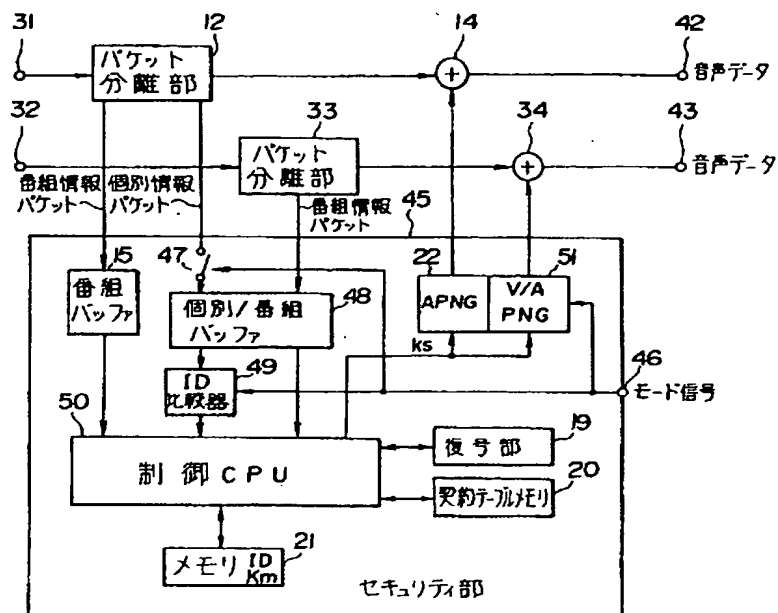
#### 4. 図面の簡単な説明

第1図は本発明に係る有料放送受信機の一実施例を示すブロック図、第2図は本発明の他の実施例を示すブロック図、第3図はスクランブル音声データを送出する送信側装置を示すブロック図、第4図は従来の有料放送受信機を示すブロック図である。

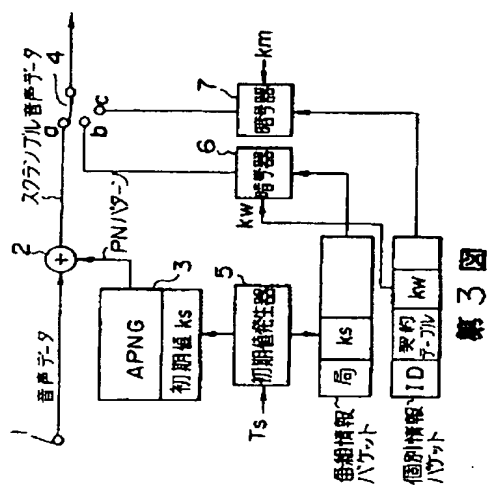
- 12, 33…バケット分離部、
- 14, 34…排他的論理和加算器、
- 15, 36…番組バッファ、19…復号部、
- 20…契約テーブルメモリ、21…メモリ、



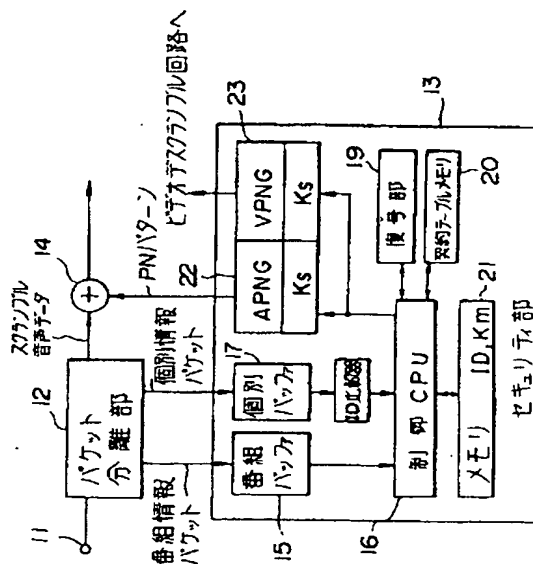
第1図



第 2 図



因  
以  
城



英寸